УДК 004.056.5

М.В. Кравчук

В.А. Гарнага

ЗАСІБ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ НА ОСНОВІ ГРАФОВОГО АНАЛІЗУ

Вінницький національний технічний університет

Анотація

У статті розглянуто підхід до побудови засобу виявлення кіберзагроз на основі графового аналізу подій інформаційної безпеки. Запропоновано архітектуру прототипу SIEM-системи, яка поєднує централізований збір логів, нормалізацію даних, правила кореляції, поведінкову аналітику та побудову графів зв'язків між сутностями. Особливу увагу приділено використанню графового представлення для виявлення прихованих взаємозв'язків між подіями, які окремо можуть не мати ознак атаки, але в сукупності формують інцидент кібербезпеки.

Ключові слова: кіберзагрози, SIEM, графовий аналіз, кореляція подій, Security Graph, Apache Kafka, Elasticsearch.

Abstract

The article considers an approach to developing a cyber threat detection tool based on graph analysis of information security events. The architecture of a SIEM system prototype is proposed, combining centralized log collection, data normalization, correlation rules, behavioral analytics, and graph-based modeling of relationships between entities. Special attention is paid to graph representation for detecting hidden relationships between events that may appear legitimate separately but together indicate a cybersecurity incident.

Keywords: cyber threats, SIEM, graph analysis, event correlation, Security Graph, Apache Kafka, Elasticsearch.

Вступ

У сучасних інформаційних системах щоденно формується велика кількість подій безпеки. Джерелами таких подій можуть бути операційні системи, сервери, мережеве обладнання, вебзастосунки, системи автентифікації та хмарні сервіси. Кожне джерело генерує власні журнали подій, які часто мають різний формат і структуру, що ускладнює їх спільний аналіз. Проблема полягає не лише у великому обсязі логів, а й у тому, що окремі події можуть виглядати легітимними. Наприклад, успішний вхід користувача до системи сам по собі не є ознакою атаки. Однак якщо перед цим було зафіксовано багато невдалих спроб входу, після входу відбулося звернення до критичного сервера, а потім − нетипова активність, така послідовність може свідчити про компрометацію облікового запису. Для вирішення таких задач застосовуються системи класу SIEM, які забезпечують централізований збір, зберігання, аналіз і кореляцію подій інформаційної безпеки. Прикладами таких рішень є Elastic Security та Wazuh, які використовуються для виявлення, дослідження та реагування на загрози [1,2]. Метою роботи є створення архітектурного фундаменту для засобу виявлення кіберзагроз на основі графового аналізу.

Основна частина

Запропонований засіб передбачає побудову прототипу системи класу SIEM, що працює за принципом модульної архітектури. Основними компонентами такої системи є колектори подій,

брокер повідомлень, модуль нормалізації, модуль аналізу, сховище даних та інтерфейс візуалізації результатів. Центральним компонентом транспортування подій є Apache Kafka. Її використання дозволяє організувати надійну передачу логів від різних джерел до модулів обробки [3]. Важливим етапом роботи засобу є нормалізація подій. Оскільки різні джерела логів можуть описувати однакові дії по-різному, дані необхідно привести до єдиного структурованого формату. До такого формату доцільно включати час події, джерело, IP-адресу, ім'я користувача, тип дії, результат виконання та рівень критичності. Це дає змогу виконувати подальший аналіз незалежно від того, з якої системи було отримано подію. Для зберігання та швидкого пошуку подій може використовуватися Elasticsearch, що є частиною екосистеми Elastic Security. Такий підхід дозволяє швидко знаходити події за користувачем, IP-адресою, часовим проміжком або типом інциденту.

Події безпеки проходять кілька послідовних етапів опрацювання. На першому етапі дані надходять від різних джерел, таких як операційні системи, мережеве обладнання тощо. Далі колектори передають події до брокера повідомлень Apache Kafka, який забезпечує надійний транспорт логів між компонентами системи. Після цього події надходять до модуля нормалізації, де приводяться до єдиного структурованого формату. Нормалізовані дані передаються до аналітичного модуля, в межах якого реалізуються правила кореляції, поведінкова аналітика та виявлення аномалій за допомогою алгоритму Isolation Forest. Результати аналізу використовуються для побудови графа зв'язків між сутностями інформаційної системи. Процес обробки подій безпеки в засобі виявлення кіберзагроз наведено на рис. 1.

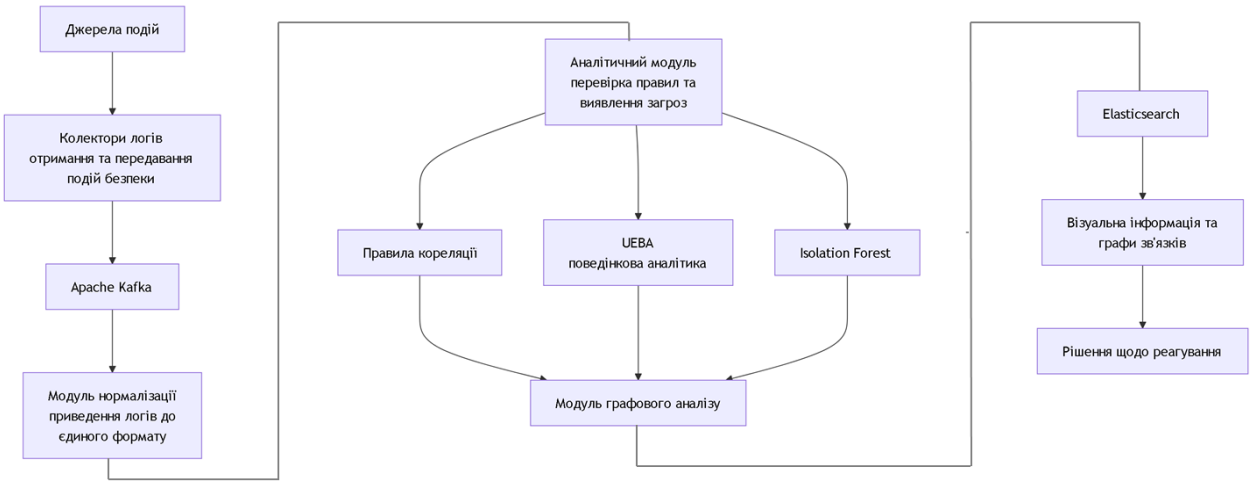

Рис. 1. Процес обробки подій безпеки в засобі виявлення кіберзагроз

Як показано на рис. 1, запропонований підхід дозволяє не лише накопичувати логи, а й аналізувати їх у взаємозв'язку, виявляти підозрілі сценарії та надавати цілісну картину можливого інциденту.

Запропонований підхід до виявлення загроз

Використовується гібридний підхід до виявлення кіберзагроз. Він поєднує детерміновані правила, поведінкову аналітику та методи машинного навчання. Наприклад, система може фіксувати багаторазові невдалі спроби входу за короткий проміжок часу, що може свідчити про Brute-force атаку. Також правила можуть використовуватися для виявлення підключень з підозрілих IP-адрес, нетипових змін прав доступу або звернень до критичних ресурсів. Поведінкова аналітика дозволяє оцінювати активність користувачів з урахуванням їхньої звичайної поведінки. Для виявлення прихованих аномалій може бути використаний алгоритм Isolation Forest. Його принцип полягає в тому, що нетипові об'єкти легше ізолюються від основної маси даних, оскільки вони мають відмінні характеристики [4]. У практичній реалізації цей алгоритм можна застосувати за допомогою бібліотеки scikit-learn, де реалізовано клас sklearn.ensemble.IsolationForest для оцінювання аномальності об'єктів [5].

Графовий аналіз подій безпеки

Ключовою особливістю запропонованого засобу є використання графового аналізу. У межах системи події безпеки розглядаються не лише як окремі записи в журналі, а як частини взаємопов'язаної структури. Для цього формується граф безпеки, у якому вершинами є сутності інформаційної системи, а ребрами − зв'язки між ними. Вершинами графа можуть бути користувачі, IP-адреси, комп'ютери, сервери, процеси, файли або інформаційні активи. Ребра відображають взаємодії між ними: IP-адреса виконала вхід до облікового запису, користувач звернувся до сервера, процес створив файл або хост встановив мережеве з'єднання. Перевага графового підходу полягає в тому, що він дозволяє виявляти складні ланцюжки атак. Окрема подія може не виглядати небезпечною, однак її зв'язок з іншими подіями може вказувати на інцидент.

Висновок

Отже, запропонована система поєднує централізований збір логів, нормалізацію подій, гібридну детекцію загроз, пошук аномалій та побудову графа зв'язків між сутностями інформаційної системи. Основна перевага такого підходу полягає у можливості виявлення прихованих взаємозв'язків між подіями безпеки. На відміну від простого аналізу окремих логів, графове представлення дозволяє розглядати інцидент як послідовність пов'язаних дій. Це особливо важливо для виявлення складних атак, у яких кожна окрема подія може виглядати легітимною, але їх сукупність вказує на загрозу. Запропонований засіб може бути використаний як основа для подальшої програмної реалізації прототипу SIEM-системи з можливістю масштабування, підключення нових джерел даних і впровадження механізмів автоматичного реагування на інциденти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Get started with Elastic Security SIEM: Detect and respond to threats. Elastic Docs. URL: https://www.elastic.co/docs/solutions/security/get-started/get-started-detect-with-siem (дата звернення: 28.04.2026).
2. Getting started with Wazuh. Wazuh Documentation. URL: https://documentation.wazuh.com/current/getting-started/index.html (дата звернення: 28.04.2026).
3. Apache Kafka Documentation. Introduction. Apache Software Foundation. URL: https://kafka.apache.org/42/getting-started/introduction/ (дата звернення: 28.04.2026).
4. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest. Proceedings of the 2008 IEEE International Conference on Data Mining, 2008. URL: https://www.lamda.nju.edu.cn/publication/icdm08b.pdf (дата звернення: 28.04.2026).
5. sklearn.ensemble.IsolationForest. scikit-learn Documentation. URL: https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.IsolationForest.html (дата звернення: 28.04.2026).

КРАВЧУК Марія Віталіївна — студентка групи 1БС-22Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: maleria002@gmail.com

ГАРНАГА Володимир Анатолійович — доцент кафедри Захисту Інформації, Вінницький національний технічний університет, Вінниця, Україна, e-mail: garnaga.volodymyr@vntu.edu.ua

KRAVCHUK Maria Vitalyivna — student of group 1BS-22b, Faculti of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

HARNAHA Volodymyr Anatoliyovych — associate professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.